CLAIMS

What is claimed is:

1 A method for electronically delivering files over a public network of computers comprising at least one server node and multiple client nodes, the method comprising the steps of:

(a) enabling secure and reliable peer-to-peer file sharing between two client nodes by,

(i) generating and associating a digital fingerprint with a file in response to the file being selected for publication on a first client node;

(ii) adding an entry for the file to a searchable index of shared files on the server node and storing the fingerprint on the server;

(iii) in response to a second client selecting the file from the search list on the server node, automatically transferring the file from the first client node directly to the second client node; and

(iv) generating a new fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity of the file and publisher.

2 The method of claim 1 further including the step of:

(b) enabling subscription-based decentralized file downloads to the client nodes by

(i) allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files,

(ii) when providing a current subscribing client node with the file, locating the closest client node containing the file, and

(iii) transferring the file from the closest node directly to the current subscribing node, thereby efficiently utilizing bandwidth.

3 The method of claim 2 wherein step (a) further includes the step of generating account information for a user, including a digital certificate, in response to a registration process, wherein the digital certificate includes a private key and a public key.

4 The method of claim 3 wherein step (a)(i) further includes the step of generating a bitstream ID for the file and including the bitstream ID in the fingerprint.

5 The method of claim 4 wherein step (a)(i) further includes the step of using the private key to generate a digital signature from the file and including the digital signature in the fingerprint.

6 The method of claim 5 wherein step (a)(iv) further includes the step of authenticating the file by generating a new bitstream ID and comparing the new bitstream ID to the bitstream ID in the fingerprint stored on the server, and using the user's public key to decrypt the digital signature.

7 The method of claim 6 wherein step (a)(ii) further includes the step of providing the server node with a database for storing the user's account information and the fingerprint for the file.

8 The method of claim 1 wherein step (a)(iii) further includes the step of transferring the file from the first client node directly to the second client node if both the first and second client nodes are logged-in to the network and no firewall separates the first and second client nodes.

9 The method of claim 8 wherein step (a)(iii) further includes the step of: if the second client node is not logged into the network, then temporarily storing the file on the server node, and delivering the file by the server node when second client node logs-in to the network.

10 The method of claim 9 wherein step (a)(iii) further includes the step of: if a firewall separates the first client node from the second client node, then using the server node to act as a proxy for the second client node and sending the file through the server node.

11 The method of claim 10 further including step (c) for allowing a user of the first client node to search for files on the network, and presorting results based on files found that are stored on client nodes located closest to the first client node.

12 The method of claim 11 wherein step (b)(iii) further includes the step of transferring the file during off-peak hours to take advantage of idle bandwidth of the subscribing node and thereby evening out bandwidth distribution of the network.

13 The method of claim 1 wherein step (a)(i) further includes the step of allowing a user of the first client node to privately publish the file or publicly publish the file.

14 The method of claim 1 wherein step (a)(ii) further includes transferring a copy of the file from the first node to the server node so that should the first node be off-line when another node request the file, the file may then be served by the server node.

15 The method of claim 1 wherein step (a)(iii) of transferring the file to the second client node further includes the step of transferring different portions of the file from different nodes and then reassembling the file upon receipt.

16 A peer-to-peer file delivery network, comprising:

at least one server node;

multiple client nodes coupled to the server node over the network, each of the client nodes running a client application, wherein the client application works and operates in conjunction with the server node to

enable secure and reliable peer-to-peer file sharing between two client nodes by,

generating and associating a digital fingerprint with a file in response to the file being selected for publication on a first client node,

adding an entry for the file to a search list of shared files on the server node and storing the fingerprint on the server,

in response to a second client selecting the file from the search list on the server node, automatically transferring the file from the first client node directly to the second client node, and

generating a new fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity and reliability of the file and publisher.

17 The network of claim 16 wherein the client application operates in conjunction with the server node to enable subscription-based decentralized file downloads to the client nodes by

allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files,

when providing a current subscribing client node with the file, locating the closest client node containing the file, and

transferring the file from the closest node directly to the current subscribing node, thereby efficiently utilizing bandwidth.

18 The network of claim 17 wherein account information is generated for a user of each client node, including a digital certificate, in response to a registration process, wherein the digital certificate includes a private key and a public key.

19 The network of claim 18 wherein a bitstream ID is generated for the file and including the bitstream ID in the fingerprint.

20 The network of claim 19 wherein the private key is used to generate a digital signature from the file and the digital signature is included in the fingerprint.

21 The network of claim 20 wherein the file is authenticated by generating a new bitstream ID and comparing the new bitstream ID to the bitstream ID in the fingerprint stored on the server, and using the user's public key to decrypt the digital signature.

22 The network of claim 21 wherein the server node includes a database for storing the user's account information and the fingerprint for the file.

23 The network of claim 16 wherein the file is transferred from the first client node directly to the second client node if both the first and second client nodes are logged-in to the network and no firewall separates the first and second client nodes.

24 The network of claim 23 wherein if the second client node is not logged into the network, the file is temporarily stored on the server node and delivered the file by the server node when second client node logs-in to the network.

25 The network of claim 24 wherein if a firewall separates the first client node from the second client node, then the server node acts as a proxy for the second client node and sending the file through the server node.

26 The network of claim 25 wherein a user of the first client node may search for files on the network, and the results are presorted based on files found that are stored on client nodes located closest to the first client node.

27 The network of claim 26 wherein the file is transferred during off-peak hours to take advantage of idle bandwidth of the subscribing node and thereby evening out bandwidth distribution of the network.

28 The network of claim 16 wherein a user of the first client node may privately publish the file or publicly publish the file.

29 The network of claim 16 wherein a copy of the file is transferred from the first node to the server node so that should the first node be off-line when another node requests the file, the file may then be served by the server node.

30 The network of claim 16 wherein different portions of the file are transferred the second client from different client nodes and then reassembled the file upon receipt.

31 A method for electronically delivering files over a public network of computers comprising at least one server node and multiple client nodes, the method comprising the steps of:

(a) enabling secure and reliable peer-to-peer file sharing between two client nodes by,

(i) generating and associating a digital fingerprint with a file in response to the file being selected for publication on a first client node,

(ii) adding an entry for the file to a search list of shared files on the server node and storing the fingerprint on the server,

(iii) in response to a second client selecting the file from the search list on the server node, automatically transferring the file from the first client node directly to the second client node, and

(iv) generating a new fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity of the file and publisher; and

(b) enabling subscription-based decentralized file downloads to the client nodes by

(i) allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files,

(ii) when providing a current subscribing client node with the file, locating the closest client node containing the file, and

(iii) transferring the file from the closest node directly to the current subscribing node, thereby efficiently utilizing bandwidth.

32 A peer-to-peer file delivery network, comprising:

at least one server node;

multiple client nodes coupled to the server node over the network, each of the client nodes running a client application, wherein the client application works and operates in conjunction with the server node to

enable secure and reliable peer-to-peer file sharing between two client nodes by,

generating and associating a digital fingerprint with a file in response to the file being selected for publication on a first client node,

adding an entry for the file to a search list of shared files on the server node and storing the fingerprint on the server,

in response to a second client selecting the file from the search list on the server node, automatically transferring the file from the first client node directly to the second client node, and

generating a new fingerprint for the file and comparing the new fingerprint with the fingerprint on the server node to determine the authenticity and reliability of the file and publisher; and

enable subscription-based decentralized file downloads to the client nodes by

allowing the client nodes to subscribe with the server node to periodically receive copies of one of the files,

when providing a current subscribing client node with the file, locating the closest client node containing the file, and

transferring the file from the closest node directly to the current subscribing node, thereby efficiently utilizing bandwidth.